

DuraMAR[®] 2150

Rugged Rolling Stock Mobile Access Router

Rev. 1.0 - December 2008 - ETH_DuraMAR2150_USM1.0

Disclaimer

The information in this manual has been carefully checked and is believed to be accurate. Eurotech assumes no responsibility for any infringements of patents or other rights of third parties, which may result from its use.

Eurotech assumes no responsibility for any inaccuracies that may be contained in this document. Eurotech makes no commitment to update or keep current the information contained in this manual.

Eurotech reserves the right to make improvements to this document and/or product at any time and without notice.

Warranty

This product is supplied with a limited warranty. The product warranty covers failure of any Eurotech manufactured product caused by manufacturing defects. Eurotech will make all reasonable effort to repair the product or replace it with an equivalent alternative. Eurotech reserves the right to replace the returned product with an alternative variant or an equivalent fit, form and functional product. Delivery charges will apply to all returned products.

Trademarks

All trademarks, both marked and not marked, appearing in this document are the property of their respective owners.

WEEE

The information below is issued in compliance with the regulations as set out in the 2002/96/CE directive, subsequently superseded by 2003/108/CE. It refers to electrical and electronic equipment and the waste management of such products.

When disposing of a device, including all of its components, subassemblies and materials that are an integral part of the product, you should consider the WEEE directive.



This symbol has been attached to the equipment or, if this has not been possible, on the packaging, instruction literature and/or the guarantee sheet. By using this symbol, it states that the device has been marketed after August 13th 2005, and implies that you must separate all of its components when possible, and dispose of them in accordance with local waste disposal legislations.

- Because of the substances present in the equipment, improper use or disposal of the refuse can cause damage to human health and to the environment
- According to WEEE, the disposal of this product with normal urban refuse is prohibited. Arrangements should be instigated for separate collection and disposal
- Contact your local waste collection body for more detailed recycling information
- In case of illicit disposal, sanctions will be levied on transgressors.

RoHS

This device, including all its components, subassemblies and the consumable materials that are an integral part of the product, has been manufactured in compliance with the European directive 2002/95/EC known as the RoHS directive (Restrictions on the use of certain Hazardous Substances). This directive targets the reduction of certain hazardous substances previously used in electrical and electronic equipment (EEE).

© 2008 Eurotech S.p.A.

Eurotech S.p.A.
A member of the Eurotech Group
Via Fratelli Solari, 3/a
33020 - AMARO (UD)
ITALY

Introduction

Conventions used within this Manual

The following conventions are used throughout this manual.

Warnings and Important Notices:

Within this manual you will find the following tables, please ensure that you read and understand these as they are intended to highlight potential risks or precautions that should be taken.



Warnings:

Warnings icons precede potentially dangerous procedures (potential personal injury or damage to a system, device, or program) throughout this manual. Instructions contained in the warnings must be followed. You should also use all other safety precautions, which you deem necessary for the operation of the equipment in your operating environment.



Information and/or Notes:

Indicates important features or instructions that should be observed

Safety Notices and Warnings

General safety precautions must be observed during all phases of operation, service, and repair of this equipment. They are listed in the Quick Reference Guide that comes with your DuraMAR-2150.

Failure to comply with those precautions or with specific warnings elsewhere in this manual violates safety standards of design, manufacture, and intended use of the equipment.

Eurotech S.p.A. assumes no liability for the customer's failure to comply with these requirements.

The safety precautions listed represent warnings of certain dangers of which Eurotech is aware.

You, as the user of the product, should follow these warnings and all other safety precautions necessary for the safe operation of the equipment in your operating environment.

Trademarks

All trademarks both marked and not marked appearing in this document are the property of their respective owners.

Warranty

This product is supplied with a limited warranty. The product warranty covers failure of any Eurotech manufactured product caused by manufacturing defects. Eurotech will make all reasonable effort to repair the product or replace it with an equivalent alternative. Eurotech reserves the right to replace the returned product with an alternative variant or an equivalent fit, form and functional product. Delivery charges will apply to all returned products.

CE Notice

This product is marked **CE** in accordance with the Class 2 product requirements specified in the R&TTE Directive, 1999/5/EC.

The CE Mark on the product indicates that the system has been tested and conforms to the provisions of the 89/336/EEC Electromagnetic Compatibility Directive and the 73/23/EEC Low Voltage Directive.

Eurotech shall not be liable for use of our products with equipment (i.e., power supplies, personal computers, etc.) that are not CE marked and do not comply with the Low Voltage Directive.

Technical Assistance

If you have a technical question or if you cannot isolate a problem with your device, please send an e-mail to the Eurotech Technical Support Team at: [email: techsupp@eurotech.com](mailto:techsupp@eurotech.com)

Before returning any Eurotech supplied product, for any reason whatsoever, you must first send an e-mail to the Technical Support Team at the above email address, providing information listed below. After this you will receive an RMA number (Returned Material Authorization) for the return of the material:

Information to be provided in RMA request:

- Model number
- Serial number
- Detailed fault description
- Company Details
- Contact details



Pack the product in anti-static material and ship it in a sturdy cardboard box with enough packing material to adequately protect the shipment.

Any product returned to Eurotech improperly packed will immediately void the warranty for that particular product!

Table of Contents

Introduction	3
Conventions used within this Manual	3
<i>Warnings and Important Notices:</i>	3
Safety Notices and Warnings	3
<i>Trademarks</i>	3
<i>Warranty</i>	3
<i>CE Notice</i>	4
Technical Assistance	4
Table of Contents	5
Chapter 1 Product Overview	7
Description	7
Architecture	8
<i>CISCO 3200 ISR</i>	8
<i>Eurotech Communications Controller (ECC)</i>	8
System interfaces	10
<i>Front panel connector layout</i>	10
<i>Rear panel connector layout</i>	11
Chapter 2 Physical Installation	13
Installation considerations	13
External Connections	14
Chapter 3 System Operation	15
Overview	15
Operation Mode	15
DuraMAR-2150 configuration	16
Command Line Interface	16
<i>User Mode</i>	16
<i>Configuration Mode</i>	17
<i>Using the no-form of commands</i>	17
<i>Using commands history</i>	18
Configuration files	18
Network interfaces general configuration	19
Ethernet interface configuration	19
HSDPA interface configuration	19
<i>Router Mode</i>	19
<i>Bridge Mode</i>	20
<i>Forcing the cellular network to use</i>	21
<i>Commands reference</i>	22
HSDPA interface information	23
Cellular network information	23
SNMP configuration	24
System administration	24
<i>Changing 'admin' user password</i>	24
<i>Limiting remote access to the system</i>	25
<i>Rebooting the system</i>	25
<i>Setting controller time and date</i>	25

<i>Setting the time zone</i>	25
<i>Log files</i>	26
<i>Setting up static routes to access external resources</i>	26
<i>Upgrading the system</i>	26
<i>Installing a new firmware using the DuraMAR USB-disk key</i>	28
<i>Using the integrated CISCO router for hosting controller system image files.</i>	29
DuraMAR-2150 service interface	30
Chapter 4 Environmental and Electrical Specs	33
Mechanical Characteristics	33
Operating Characteristics	33
Absolute Maximum Ratings	34
Compliance	34
Revision History	35
Eurotech Group Worldwide presence	37

Chapter 1 Product Overview

Description

The DuraMAR® 2150 is a rugged integrated wireless router designed for providing net-centric connectivity in rolling stock installations such as on trains and metros.



Figure 1. Picture of the DuraMAR-2150

Key features include:

- Compliance with train and rail standards, EMC, EMI, shock and vibration
- Extended operating temperature range: -20°C / $+55^{\circ}\text{C}$ (70°C for 10 minutes) EN50155 class T1
- Wide storage temperature range: -20°C up to 70°C EN50155 class T1
- Conduction cooled system
- Solid state system storage, 512 MB Flash Disk
- Rugged mechanical construction
- IP65 ingress protection
- Rugged locking circular connectors with strain relief
- Nominal 110Vdc train feeder supply

Architecture

The DuraMAR-2150 system consists of:

- a CISCO 3200 series Integrated Services Router (ISR) core running the industry standard IOS® software
- a Eurotech Communication Controller (ECC) featuring an integrated high speed wireless HSDPA interface

CISCO 3200 ISR

Cisco® 3200 Series wireless and mobile router offers secure data, voice and video communication. It supports multiple wired and wireless links, including integrated 802.11b/g and 4.9-GHz wireless technologies. With a flexible, compact form factor, these rugged router cores are ideally suited for integration in vehicles or installations outdoors. Standard Mobile IP services provide transparent roaming in wireless networks for mobile installations. The Cisco IOS® Software includes data security, manageability, and scalability, along with interoperability between networks, while supporting new and evolving network and wireless technologies.

The CISCO 3200 ISR core of the DuraMAR-2150 includes:

- Mobile Access Router Card (MARC)
- Fast Ethernet Switch Mobile Interface Card (FESMIC)

Eurotech Communications Controller (ECC)

The Eurotech Communication Controller interfaces the CISCO 3200 ISR core with various wireless terminals such as GPRS, UMTS, HSDPA, HSUPA or CDMA2000 using a 10/100Mbit Ethernet interface. The use of industry-standard mini PCI-Express form wireless terminals guarantees an easy upgrade path to adopt new technologies with the change of only a single module.

The core of the Eurotech Communications Controller subsystem consists of the following parts:

- Eurotech CPU-1452 (standard x86 architecture)
- System carrier including power supply, HSDPA and GSM/GPRS modems

HSDPA Section

The Sierra Wireless MC8775V HSDPA module is mounted within the system.

HSDPA features:

- Tri-band UMTS/HSDPA: 850/1900/2100 MHz
 - Downlink up to 7.2 Mbps
 - Uplink up to 1 Mbps
- Power Class: 3 (+24 dBm)

EDGE features:

- Quad-band EDGE/GPRS/GSM: 850/900/1800/1900 MHz
 - Downlink up to 216 kbps
 - Uplink up to 108 kbps
- GSM Power Class 4 for 850 / 900 bands, GSM
- Power Class 1 for 1800 / 1900 bands
- EDGE class E2

GSM/GPRS Section

A Siemens MC55 GSM/GPRS modem is mounted within the system.

GSM/GPRS features:

- Support for Tri-band GSM/GPRS networks 900/1800/1900MHz bands
- Up to 56Kbps GPRS data rate depending on network bandwidth
- GPRS downlink data rate up to 85.6kbps
- Full SMS support
- GPRS mobile station class B and multi-slot class 10 compliant
- Output power: 2W for EGSM900 and 1W for GSM1800/1900
- Approvals: R&TTE, FCC, IC, GFC, PCCRB and local approvals as well as mobile operator certifications
- Interfaces to the system CISCO/controller through a serial port

Power supply subsystem features

The DuraMAR-2150 power supply subsystem features include:

- Input power filtering and protection circuitry with high power tranzorb over-voltage protection diodes
- Isolated train qualified DC/DC converter with post regulators providing power to all system devices
- Reverse voltage protection up to –200VDC

The system can be powered directly from a train feeder supply:

- Nominal power supply: 110VDC
- Typical power consumption: < 44W

Warning:

Electric current from power and communication cables is hazardous. To avoid shock hazard when connecting or disconnecting cables, follow appropriate safety precautions. Ensure that the correct operating voltage is used when powering the device.



Danger
110 Volts

System interfaces

Front panel connector layout

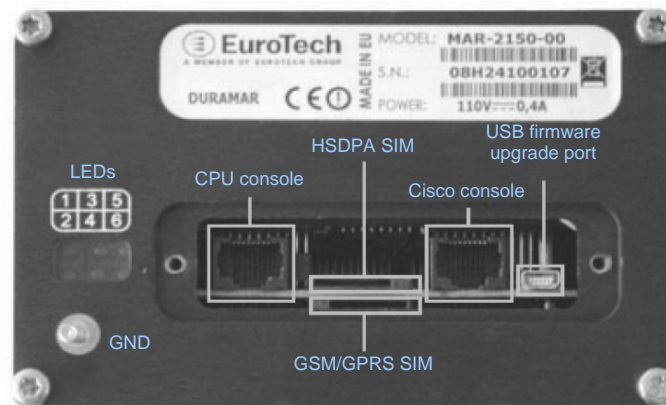


Figure 2. Front panel layout (with protection cover removed)

Service interfaces

Some service interfaces are provided on the front panel of the system under a protection cover. It is possible to remove this cover by removing the two Torx screws.



Warning:

While the protection cover is removed it is not possible to maintain the IP protection grade

The service interfaces can be used for debugging, firmware uploading, system configuration and diagnostics:

- SIM card holder for HSDPA
- SIM card holder for GSM/GPRS
- CISCO 3200 ISR serial console port
- ECC serial console port
- USB1.1 port of embedded controller for firmware upgrading

LED indicators

On the front panel of the system there are 6 LED indicators with functions as described below.

LED Number	Function	Comments
1	Not Connected	-
2	Power Good	+12 V present
3	GSM activity	Software programmable
4	HSDPA activity	Software programmable
5	Power #1 On	5 V present
6	Power #2 On	3.3 V present

Rear panel connector layout

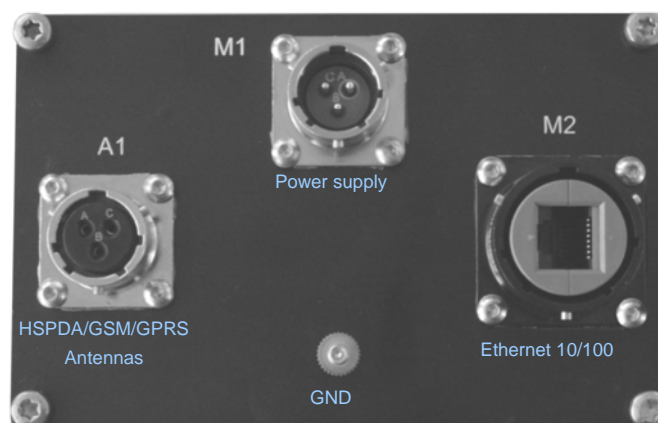
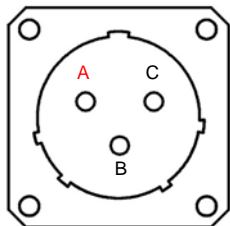


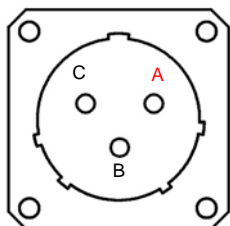
Figure 3. Rear side connector layout

Connector	Type	Function availability
A1	Connector: <ul style="list-style-type: none"> Receptacle MIL-26482 coaxial; 3-pin; shell size 12 P/N: Souriau MS3470L12-3BN Coaxial Contact #16 for cable RG174A/U P/N: Souriau 8526-1-001A 	<ul style="list-style-type: none"> HSDPA Antenna GSM/GPRS Antenna
	Mating with: <ul style="list-style-type: none"> Plug MIL-26482 series; 3-pin; shell size 12 P/N: Souriau 851-02E-1203P5044 	
M1	Connector: <ul style="list-style-type: none"> Plug MIL-26482 series; 3-pin; shell size 12 P/N: Souriau 851-02E-1203P5044 	<ul style="list-style-type: none"> 110Vdc nominal input power
	Mating with: <ul style="list-style-type: none"> Receptacle MIL-26482; 3-pin; shell size 12 P/N: Souriau 851-06RCI2-0355044 	
M2	Connector: <ul style="list-style-type: none"> Receptacle MIL-26482; RJ45; shell size 12 P/N: Amphenol RJF22N00. 	<ul style="list-style-type: none"> Ethernet 10/100 Mbps
	Mating with: <ul style="list-style-type: none"> Plug MIL-26482; RJ45; shell size 12 P/N: Amphenol RJF6MN. 	
GND	<ul style="list-style-type: none"> Grounding terminal for an M4 ring Faston connector 	<ul style="list-style-type: none"> Allows the connection of the system chassis to the chassis ground of the installation.

Table 1. Connector definitions

A1 pinout

Pin#	Signal
A	HSDPA Antenna
B	GSM/GPRS Antenna
C	Not internally connected

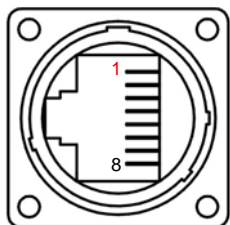
M1 pinout

Pin#	Signal
A	VIN+
B	Not internally connected
C	VIN-

**Note:**

These inputs are galvanically isolated from the system.

VIN- is not connected to the system ground nor to the chassis.

M2 pinout

Pin#	Signal
1	TX+
2	TX-
3	RX+
4	Unused
5	Unused
6	RX-
7	Unused
8	Unused

Chapter 2 Physical Installation

Physical installation may only be performed by trained and authorized personnel. The electrical installation must adhere to local regulation requirements. The instructions for use must be followed at all times.

Installation considerations

- The device must not be accessible to passengers nor operational staff (excluding maintenance).
- The unit must be placed such that there is sufficient space for connecting the cables and removing the protection cover.
- A minimum clearance of 50mm around the device should be ensured in order to avoid possible overheating. The space required by the connectors and cables can be up to 90mm, therefore sufficient space should be reserved for installing the system.
- The device must be secured firmly. A device that is inadequately fixed may cause danger to people or other equipment in the vehicle. The safety instructions of the vehicle must be followed rigorously.
- The device must be mounted inside an appropriate equipment cabinet.
- The device can be fixed in any orientation (vertical, transversal and longitudinal)

The DuraMAR-2150 anodized enclosure is built from two extruded aluminium parts. The outside dimensions excluding connectors are:

Length (mm)	Width (mm)	Height (mm)
254	129	83

Square nuts (as shown in the diagram below) are mounted within slots on the system casing and therefore can be positioned in a location to best suit the customer's requirements.

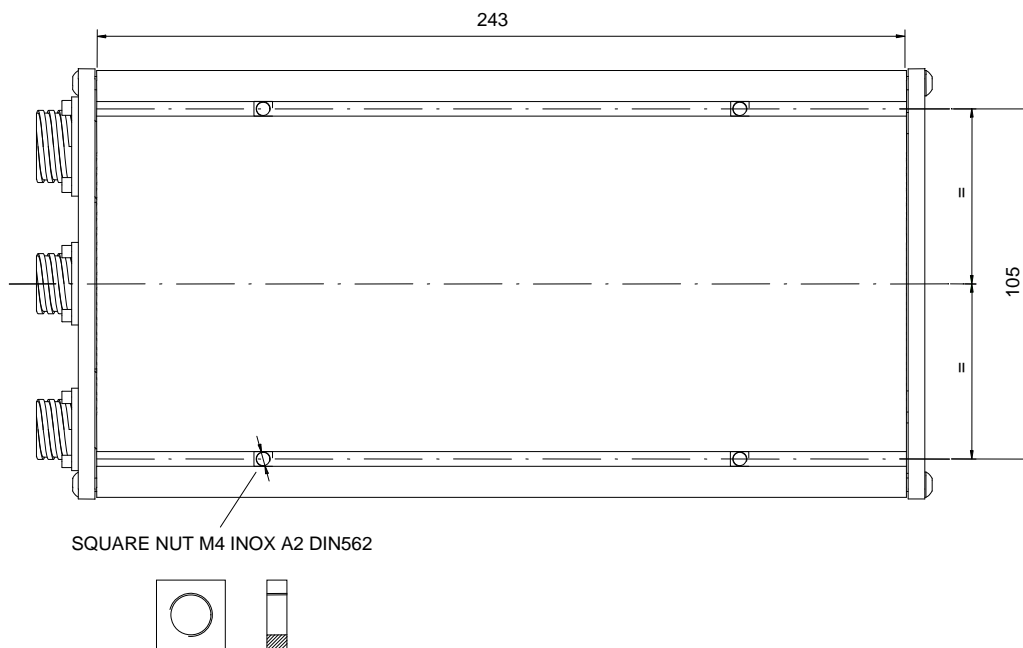


Figure 4. Slots and Square nuts dimensions (mm)

External Connections

Only devices that meet SELV circuits (Security Extra Low Voltage) requirements in accordance with the EN60950 standard should be connected to the interfaces of the DuraMAR-2150.

All connection cable plugs must be screwed or locked to the housing.

To maintain the Protection class, the connectors of the external cable must be adequately sealed and every unused connector must be covered.

Ensure that all connected cables, particularly the power cables, are positioned in areas where people or machinery do not risk entanglement or being hit by the system.

Vehicle power should only be connected after the installation of the system has been completed.

All unused cables should be isolated or removed if possible.

The cables must be shielded and the shields have to be grounded on both sides.

The system must be grounded using the connection terminal in Rear Panel with the shortest possible connection (max 20cm) using a low resistance cable.



Warning:

Electric current from power and communication cables is hazardous. To avoid shock hazard when connecting or disconnecting cables, follow appropriate safety precautions. Ensure that the correct operating voltage is used when powering the device.



Danger
110 Volts

Chapter 3 System Operation

This chapter illustrates the operation of the Eurotech Communication Controller (ECC) and its interaction with the CISCO 3200 ISR. If not otherwise stated, hereafter the word “*system*” will implicitly refer to ECC subsystem only.

Overview

The ECC is a standard x86-based system running a Linux kernel and a preinstalled application software (hereafter referred to as *ECC firmware*).

The ECC firmware provides a command line interface by which the user can obtain status information and perform configuration and maintenance operations. Available status information includes: network interface status, signal quality, availability of HSDPA service, internal temperatures as well as CPU parameters such as memory usage and CPU load. Some of this information can be also accessed using SNMP protocol.

The system is equipped with three different network interfaces:

- one 10/100 Mbps Ethernet interface (eth0)
- one 3G cellular interface (hsdpa0) used for providing HSDPA connectivity to the CISCO 3200 ISR
- one 2G cellular interface (gprs0) available as a backup interface for accessing the system in case of failure on the 3G interface

Operation Mode

The system is capable of operating in two modes:

- Routing Mode
- Bridging Mode

The mode of operation depends on the configuration of the HSDPA interface (see [further](#)).

Routing mode

In *Routing mode* the ECC operates as a standard router connected to the CISCO 3200 ISR with an Ethernet link. In this mode a couple of private IP addresses are used on the link between ECC and the CISCO 3200 ISR with NAT (Network Address Translation) translation enabled on the wireless HSDPA interface.

This mode is suitable when there is no special requirement for the IP address used on the CISCO 3200 ISR router interface.

Bridging mode

In *Bridging Mode* the ECC will pass the carrier-assigned public IP address back to the CISCO 3200 ISR and assumes an address in the same subnet for preserving IP connectivity. This public IP address can be statically assigned to the CISCO 3200 ISR interface or made dynamically available using the DHCP protocol.

This mode is suitable for installations where a single public IP address negotiated on the wireless HSDPA link must be made available on the CISCO 3200 ISR router interface.

DuraMAR-2150 configuration

The configuration of DuraMAR-2150 system involves the configuration of the CISCO 3200 ISR and ECC subsystems.

- The CISCO 3200 ISR subsystem can be configured using the console interface available on the panel side under the removable protection cover. The serial communication parameters must be set to 9600N81 (9600 baud, No parity, 8 bit data size, 1 Stop bit). There is no username or password defined in the default configuration. Please refer to the documentation provided by CISCO for detailed configuration of the CISCO 3200 ISR devices.
- The ECC subsystem can be configured using the console interface available on the front panel under the service panel. The serial console communication parameters must be set as 115200N81 (115200 baud, No parity, 8 bit data size, 1 Stop bit).

Command Line Interface

The Command Line Interface (CLI) is a text-based user interface that provides a set of commands to configure the settings and monitor functions and status of the system. These commands and the way the CLI is used is very similar to the CISCO IOS® command interface making the use of CLI easy to adopt for experienced CISCO IOS® users.

The CLI is available to the user by connecting a terminal emulator to the serial console port interface (the one under the service panel) or by accessing the system through a SSH session. In both cases to access the CLI the user is asked to provide the following login information:

- username: *admin*
- password: *admin* (default)

Once logged in, the user enters to a CLI *session*. The CLI will show a prompt and will wait for user input. The session is terminated when the user logs out.

A help command ('?') is available at any time for a list of available commands or the required parameters that must be typed as arguments of a given command.

The CLI uses two different modes of operation:

- User Mode
- Configuration Mode

User Mode

Logging in to the device places the user in *User Mode*. In this mode the prompt consists of the host name assigned to the system followed by a pound sign (#), as shown in the following example:

```
HSDPA-rt#
```

The default host name is empty so the initial prompt will be composed only of the pound symbol (#). The host name can be changed issuing the `hostname` command.

To view the list of commands available in this mode, the user can type a question mark as shown in the following example:

```
HSDPA-rt# ?
Show      Show running system information
Configure Enter configuration mode
Copy      Load or save configuration
Debug     Enable debugging information on terminal
Undebug   Disable debugging information on terminal
Exit      Exit from the cli
```

Configuration Mode

The *Configuration Mode* is used to configure the system. This mode provides two sub-modes of operation: *Global* or *Specific*, depending on what part of the system the user is configuring. *Specific* mode allows access to the configuration area of one of the system components, hardware or software, while *Global* mode allows access to global configuration parameters affecting the whole system.

To enter the Configuration Mode from User Mode issue the command: `configure`. When entering Configuration Mode you will find yourself in Global configuration mode.

The system prompt changes to indicate that now you are in *Global* configuration mode as shown below:

```
HSDPA-rt(config)#
```

Commands entered in Configuration Mode update the running configuration immediately, as soon as the command is entered. However, these changes are not saved in the start-up configuration file until you issue the `copy running User mode` command to save the configuration.

Entering a string identifying a specific system component while in Configuration Mode makes the user enter the Specific configuration mode. Commands available in this mode are specific for the component you are configuring.

As an example, to configure the Ethernet interface (`eth0`), you will issue the command `interface eth0`. Entering this command moves you to the specific configuration mode of the selected component and the prompt changes accordingly as shown in the following example below:

```
HSDPA-rt(config)# interface eth0
HSDPA-rt(config-if-eth0)#
```

While in Specific configuration modes such as in the example above, the commands available are only related to the specific component as shown below:

```
HSDPA-rt(config-if-eth0)# ?
description  Interface description
IP           IP Protocol config commands
enable       Enable the selected interface
mobile       Enable mobile subsystem on this interface
mtu          Change the mtu size for this interface
nat          Enable NAT services on this interface
exit        Exit from interface configuration mode
```

To exit from Specific configuration mode thus returning to Global configuration mode use the `exit` command. To end the configuration session issue the `exit` command from Global configuration mode.

Using the *no-form* of commands

Almost every configuration command has a *no-form* that is used to reset or disable the specific configuration parameter/value.

For example the following commands:

```
HSDPA-rt(config-if-eth0)# enable
HSDPA-rt(config-if-eth0)# no enable
```

will first enable (or activate) and then disable (or deactivate) the Ethernet interface.

As another example, the following commands:

```
HSDPA-rt(config)# route 192.168.10.0 255.255.255.0 via 10.11.3.1
HSDPA-rt(config)# no route 192.168.10.0 255.255.255.0
```

will first set up a static route and then remove it.

Using commands history

The CLI stores a history of commands that you have entered. This feature is particularly useful for recalling long or complex command or entry strings. In order to recall commands from the command history buffer, use the up and down arrows keys. The history is **not preserved** across CLI sessions.

Configuration files

The configuration file looks like a plain text file that contains the commands used to define the functionality of the system. The commands included in the configuration file are executed automatically when the system is powered-on or when the user enters a command from the CLI in Configuration Mode.

There are two different types of configuration files:

- a start-up configuration file that is used during system start-up to configure the controller and that is stored in a non-volatile memory
- a running configuration file that contains the current active configuration

These two configuration files can be different. Configuration changes persist across CLI sessions, but will not be recorded in the start-up configuration file and will be lost as soon as the system is rebooted or switched off. To preserve the changes the user must save the running configuration on the system non-volatile memory using the `copy running` command while in User mode.

The user can also save the running configuration to a file using the `copy running file_name` command and reload it later using the `copy file_name running` command.

The user can switch between different configuration files using the `copy file_name startup` command.

The complete syntax of the `copy` command is the following:

<code>copy running</code>	Copies current running configuration to the start-up configuration file
<code>copy startup</code>	Loads the current start-up configuration file on to the current running configuration
<code>copy running file_name</code>	Copies the current running configuration file to the specified file
<code>copy file_name running</code>	Copies the specified configuration file on to the current running configuration
<code>copy file_name startup</code>	Copies the specified configuration file on to the start-up configuration file

The contents of the running or the start-up configuration file can be examined by issuing the `show running` and `show startup` commands, respectively.

Network interfaces general configuration

To configure a network interface the user must enter the *Specific Configuration Mode* for the given interface by issuing the `interface if-name` command while in *Configuration Mode*. The prompt will change accordingly.

For example:

```
HSDPA-rt(config)# interface hsdpa0
HSDPA-rt(config-if-hsdpa0)#
```

The list of available interfaces can be obtained by issuing the `show interface` command.

Ethernet interface configuration

To configure the Ethernet interface the user must perform the following steps:

1. `configure`
2. `interface if-name`
3. `ip address ip-address [mask] [link-gw]`
4. `enable`

If you don't specify any net-mask the system will use a standard class net-mask based on the IP address itself. The `link-gw` parameter is the IP address of the gateway used for outgoing traffic from this interface.

The available commands for configuring the Ethernet interface are the following:

description	Adds a text description for the interface
ip address addr [mask] [link gw]	Assigns an IP address to the interface
mtu	Sets the IP Maximum Transmit Unit (MTU)
tcpmss	Forces the TCP Maximum Segment Size for the sessions entering or exiting from the interface
nat	Enables Network Address Translation. The source address of all of the packets sent out through this interface will be changed to the IP address assigned to the interface itself
enable	Activates the specific interface

HSDPA interface configuration

The configuration of the HSDPA interface affects the system's operation mode.

Router Mode

In Router Mode the system operates as a standard router: all the traffic that comes in from the Ethernet interface is routed through the 3G wireless link.

To configure the system for operating in Router Mode, the `hsdpa0` interface must have the NAT service enabled and must be used as default route for the outgoing traffic. The IP connectivity between the CISCO 3200 ISR and the ECC must be properly configured and the IP address assigned to the `eth0` interface of the ECC must be configured as default gateway on the CISCO 3200 ISR.

The steps required to configure the interface for Router Mode are as follows:

1. `configure`
2. `interface if-name`
3. `apn network_name`
4. `default route`

5. nat enable
6. enable
7. exit
8. exit

Please note that the exit command must be issued twice.

An example of a Router Mode configuration follows:

```
Version: 1.0.0 - $Rev: 317 $
!
hostname HSDPA-rt
interface eth0
    ip address 172.16.10.1 255.255.255.252
    enable
!
interface hsdpa0
    ip address negotiated
    enable
    apn web.omnitel.it
    mode auto
    default route
    nat enable
```

The CISCO 3200 ISR must be configured accordingly as in the example below:

```
!
interface FastEthernet0/0
ip address 10.200.1.24 255.255.0.0
duplex auto
speed auto
!
.....
!
.....
!
interface FastEthernet1/3
!
interface Vlan1
ip address 172.16.10.2 255.255.255.252
!
!
ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

Note that the FastEthernet 1/3 interface is a switched interface so the IP address must be assigned to a VLAN interface and can't be directly assigned to the Ethernet interface as for fa0/0 (which is a fully routed interface).

Bridge Mode

In *Bridge Mode* the system will pass the carrier-assigned public IP address of HSDPA interface back to the CISCO 3200 ISR allowing the latter to use this address as it was directly assigned to its Ethernet interface.

The steps required to configure the interface for Bridge Mode are:

1. configure
2. **interface** *if-name*
3. **apn** *network_name*
4. **pppbri dge** *if-name* **dynamic** | **static**
5. enable
6. exit
7. exit

Bridge Mode can be *dynamic* or *static*.

Dynamic Bridge Mode

In Dynamic Bridge Mode the carrier-assigned public IP address is made available to the CISCO 3200 ISR FastEthernet interface using the DHCP-protocol; then the first (.1) or last (.254) IP address of the network that this address belongs to is automatically assigned to the ECC Ethernet interface in order to guarantee local IP-connectivity.

For example if the carrier assigns 114.22.34.2 to the PPP connection this address will be made available to the CISCO 3200 ISR using DHCP and the address 114.22.34.1 will be assigned to the ECC eth0 interface. In this case DHCP responses will contain 114.22.34.1 as default gateway.

Dynamic Bridge Mode is the default mode and must be used when the IP address assigned by the wireless provider is not fixed but can change from one connection to another.

An example of a Dynamic Bridge Mode configuration follows:

```
! Version 0.1
!
hostname myhost-hsdpa
!
interface eth0
no IP address
enable
!
interface hsdpa0
IP address negotiated
apn myhost
pppbridge eth0 dynamic
enable
!
```

Note that, with this configuration, the eth0 interface can't have an IP address assigned.

The CISCO 3200 ISR must be configured accordingly as in the example below:

```
!
interface FastEthernet0/0
ip address 10.200.1.24 255.255.0.0
duplex auto
speed auto
!
.....
!
interface FastEthernet1/3
!
interface Vlan1
ip address dhcp
!
!
```

Note that in this case the IP address of vl an1 interface is dynamically assigned by the DHCP server.

Static Bridge Mode

Static Bridge Mode should be used when the carrier-assigned public IP address is fixed. In this case, there is no need to use the DHCP-protocol, while the fixed address can be directly configured to the CISCO 3200 ISR Ethernet interface and the IP address assigned to the eth0 interface of the HSDPA controller must be chosen and configured by the user. This address must also be defined as default gateway on the CISCO 3200 ISR.

Forcing the cellular network to use

By default the hsdpa0 interface automatically uses the 2G (GSM) or 3G (WCDMA) network depending on the quality of the signal.

You can force the device to use only 2G or only 3G networks using the mode command.

Commands reference

The following table lists the available commands for configuring the HSDPA interface:

descri ption	Adds a text description for the interface
mtu	Sets the IP Maximum Transmit Unit (MTU)
tcpmss	Forces the TCP maximum segment size for the sessions entering or exiting from the interface
default route	The interface will be used as default gateway
apn <i>network_name</i>	Defines the Access Point Name (APN) for the PDP context
username <i>username</i>	Username to use during authentication. Do not use this if the wireless operator does not require any authentication
password <i>password</i>	Password to use for authentication. Do not use if the wireless operator does not require any authentication
pppbridge <i>ifname</i> [static dynamic]	Enables bridge service on this interface. <ul style="list-style-type: none">• <i>bridge static</i> performs the proper setup of the PPP link. The Ethernet interface of the controller and of the router must be manually configured• <i>bridge dynamic</i> performs the proper setup of the PPP link and makes the public IP address from the wireless provider available to the router interface using DHCP protocol. The IP address of the router should be configured to use DHCP
nat	Enables Network Address Translation on outgoing traffic. The source address of all of the packets sent though the PPP link will be changed to the address of the PPP link itself. Function not available if <i>bridge dynamic</i> is used
mode [auto 2G 3G]	Forces the type of cellular network to be used
enabl e	Activates the specific interface

HSDPA interface information

The current status of the HSDPA interface can be retrieved using the `show interface hsdpa0` command in *User Mode*:

```
HSDPA-rt# show interface hsdpa0
Interface hsdpa0 is Enabled physical status is PPP up
Hardware type is HSDPA modem
Network in use : HSDPA Cat. 6 (3.6Mbps)
IP address is 91.80.172.179 255.255.255.255
Link gateway is not set
MTU 0 bytes qdisc is
```

From the output of this command the user will know: the interface status (*enabled* or *disabled*), the PPP link status (*up* or *down*), the IP address provided by the ISP and the type of network in use (*GPRS* if 2G or *UMTS*, *EDGE* or *HSDPA* for 3G networks).

Cellular network information

You can get detailed information about the current status and availability of the cellular network for the `hsdpa0` interface issuing the command `show modem status` in *User Mode*.

From the output of this command the user can know almost everything about the status of network registration.

Here is an example of the output of this command in a good 3G coverage area:

```
HSDPA-rt# show modem status
Current status for modem interface hsdpa0
Current Time: 131566 Temperature: 50
Bootup Time: 57997 Mode: ONLINE
System mode: WCDMA PS state: Attached
WCDMA band: IMT2000 GSM band: Unknown
WCDMA channel: 10564 GSM channel: 65535
GMM (PS) state: REGISTERED NORMAL SERVICE
MM (CS) state: IDLE NORMAL SERVICE

WCDMA L1 State: L1M_DCH RRC State: CELL_DCH
RX Level (dBm): -70
```

This is the output of the `show modem status` command in an area with no 3G coverage:

```
HSDPA-rt# show modem status
Current status for modem interface hsdpa0
Current Time: 8904 Temperature: 47
Bootup Time: 2 Mode: ONLINE
System mode: WCDMA PS state: Attached
WCDMA band: IMT2000 GSM band: GSM900
WCDMA channel: 10638 GSM channel: 65535
GMM (PS) state: REGISTERED LIMITED SERVICE
MM (CS) state: IDLE LIMITED SERVICE

WCDMA L1 State: L1M_PCH_SLEEP RRC State: DISCONNECTED
RX Level (dBm): -104
```

Note the LIMITED SERVICE values for GMM and MM fields and the DISCONNECTED RCC state.

The relevant fields in the output of this command are:

Temperature	The internal temperature of the ECC HSDPA module
System mode	GPRS (2G) or WCDMA (3G)
GMM and MM state	NORMAL SERVICE or LIMITED SERVICE
RCC_STATE	The registration status, CELL_DCH, CELL_FACH, DISCONNECTED (for 3G networks only)
RX level	The quality of the signal received by the module

SNMP configuration

The system can be monitored using the SNMP protocol. Only SNMP version 2c is supported. The available information includes:

- the current 3G network type used by the hsdpa0 interface
- the signal quality on the hsdpa0 interface
- the internal temperature of HSDPA modem
- the internal temperature of CPU

SNMP traps are sent to the configured manager host if the temperatures of the HSDPA module or the CPU exceed a predefined fixed value and whenever there is a change on the 3G network type.

The basic configuration of the SNMP agent requires only the definition of a *community name* and the enabling of the service. Here are the required steps:

1. `configure`
2. `snmp-server community private`
3. `snmp-server enable`
4. `exit`

The complete list of commands available for the SNMP agent configuration is listed below:

<code>snmp-server community <i>string</i></code>	Sets the community name (<i>this is a mandatory step</i>)
<code>snmp-server contact <i>string</i></code>	Sets the contact name
<code>snmp-server location <i>string</i></code>	Sets the locations of the device
<code>snmp-server name <i>string</i></code>	Sets the logical name of the device
<code>snmp-server host <i>ip-address</i></code>	Sets the IP address of the management station
<code>snmp-server enable</code>	Enables the SNMP agent service

You can view the SNMP server status and configuration issuing the `show snmp-server` command.

System administration

Changing 'admin' user password

The user can change the password that is used to protect the *admin* user login.

While in Configuration Mode, the `passwd` command is used to perform the change. The user will be asked for the new password to be assigned to the admin user. The password is not echoed on the screen for security reasons. Moreover, the `passwd` command is not shown in either running or start-up configuration files.

Limiting remote access to the system

Access to the system by connecting through the gprs0 interface can be restricted to a list of specific IP addresses. There are no limits to the number of IP addresses in the list.

By default there is no access restriction. By issuing one or more `set admin-ip ip-address` commands the user can restrict the access to only the given IP addresses.

The *no-form* of the command removes the permission. If the list is empty, the access will be automatically granted from any IP address.

Here is an example that allows access from just two IP address:

```
!
set admin-ip 217.22.11.23
set admin-ip 217.22.11.24
!
```

These restrictions apply to any kind of IP traffic coming from an IP address that is not included in the list, thus also SSH, SNMP and ICMP packets will be rejected.

Rebooting the system

An immediate reboot of the ECC system can be performed by issuing the `reboot` command. Please note that this command will reboot ECC only, while CISCO 3200 ISR subsystem will not be affected.

Setting controller time and date

The user can setup the controller time and date using the `set time` configuration command.

There is no internal battery for maintaining the system's clock so, if the device is powered off for a couple of hours or more, the time will be lost.

If you need or want to maintain a precise system time you can keep the system clock in sync with up to three external NTP (Network Time Protocol) servers using the `set ntp` configuration command. Please note that when the system operates in Bridge Mode, one or more static routes need to be defined for this feature to work (see further for details)

The complete list of commands available for managing system time:

<code>show time</code>	Displays the current time and date
<code>set time hh:mm[:ss] mm/dd/yyyy</code>	Sets the current time and date values
<code>set ntp <ip-address> [ip-address ip-address]</code>	Defines up to three NTP servers

Setting the time zone

The internal clock is typically maintained in UTC coordinates. You can define the time zone in which the system is used using the `set tz` configuration command.

The time zone is expressed defining the name of a geographical area (ie. Europe, Asia,...) followed by the name of a city in that area (ie. Rome, Singapore,...). A question mark (?) can be used in place of the zone or city names, to obtain a list of these fields.

The syntax of this command is:

```
set tz <area name> <city name>
```

Log files

Important events are logged on the flash memory. User can view the logged messages using the `show log` system command. Because the size of the flash memory available for the log file is limited, the size of the log file is checked periodically and, if it increases to more than 3MB, it is automatically resized to the last 1000 messages. At any moment user can clear the log file using the `delete log` configuration command.

Log messages can also be saved on a remote *syslog* server using the `set log` command. Please note that when the system operates in Bridge Mode, one or more static routes need to be defined for this feature to work (see further for details).

The complete list of commands available for managing log files:

<code>show log</code>	Displays the contents of the log file
<code>clear log</code>	Removes all of the log messages
<code>set log <ip-address></code>	Defines the IP address of a remote syslog server

Setting up static routes to access external resources

In order to access an external resource (such as a NTP or *syslog* server) when the system operates in Bridge Mode, the user must define one or more static routes through the `gprs0` interface. This is required because in Bridge Mode the system can only forward traffic to the default route (the `hsdpa0` interface). The syntax is:

```
route ip-address netmask dev gprs0
```

where *ip-address* and *netmask* are, respectively, the IP address and network mask of the external resource destination.

Upgrading the system

ECC firmware can be upgraded using the `upgradefrom` command. This command will download a new system image from a specific URL and automatically install it. For example:

```
HSDPA-r(config)# upgradefrom http://212.12.54.21/hymar-1.1.eff
```

An updated version of the controller firmware can be easily downloaded and installed from a remote HTTP or FTP server.

The upgrade process is a three-step procedure:

- the image file is downloaded alongside with some information that checks its integrity (an MD5 digest contained in a plain text file)
- the image file is processed for integrity check comparing the MD5 digests
- the new valid image is saved on the flash memory and the default start-up configuration file is updated accordingly

The `upgradefrom` configuration command performs all of these steps automatically. The syntax is the following:

```
upgradefrom <URL-address>
```

At the end of the upgrade process the system must be rebooted without issuing the `copy running` command. This is important because the upgrade procedure updates the content of the startup configuration but not the content of the running configuration. Issuing the `copy running` command will overwrite the correct configuration.

If needed the upgrade process can be performed manually with the following steps.

First the new firmware image must be downloaded, verified and saved to the flash memory. This can be done using the `download image` command. This command will download the new image, check it's correctness and save it to the flash memory. The syntax is the following:

```
download image <URL-address>
```

Then the user should configure the system so that it will boot the new image at next reboot, using the `boot system` configuration command. The syntax is the following:

```
boot system <image file name>
```

This command changes only the running configuration so, in this case, the user must issue the `copy running` command before rebooting the system.

The `boot system` command can be used at any time for selecting one of the firmware images available on the flash disk as the system boot image. The list of images saved on the flash can be obtained using the `show boot-images` command, while old images can be removed using the `delete boot-image` configuration command. This command can be used to free space on the flash memory thus providing room for new images. The image installed by the manufacturer can't be removed and is reported as default image and it will be used if `boot system` command is removed from the configuration file.

The complete list of commands available for managing the system image files is listed below:

<code>upgrade from <URL-address></code>	Downloads and installs a new system image. At the end the system must be rebooted without issuing a copy running command
<code>download image <URL-address></code>	Downloads and saves on the flash memory a new system image file.
<code>boot system <image-file></code>	Defines the image file to boot from. This is a configuration command so user must save the running configuration for saving the changes.
<code>show boot-images</code>	Displays a list of the system image files currently on the flash memory,
<code>delete boot-image <image-file></code>	Removes from the flash memory the specified system image file.

URL address format

The address where a new system image can be downloaded is defined using a standard URL (Uniform Resource Locator) address:

```
protocol://[username:password@]ip-address/file_name.eff
```

The protocols supported are HTTP and FTP, the remote server must be referred to using its IP address instead of its name because the system is not capable of resolving DNS names.

System upgrade can also be performed via remote SSH connection. From a remote system issue the command:

```
ssh admin@controller_IP upgrade from url
```

Installing a new firmware using the DuraMAR USB-disk key

Whenever the system doesn't boot as expected (for example in case some system file has become corrupted or unreadable) or whenever a new fresh installation is required, the user can install the firmware by using the provided USB-disk key. This operation is not intended to be performed as routine maintenance but only in case of serious problems.

The DuraMAR USB-disk key contains maintenance software that performs a series of operations, including setting up the system storage memory layout and installing the firmware image contained in the USB-disk key itself. The status of the process can be monitored through the serial console. **This process erases all the data already present on the ECC and sets-up the system with factory defaults.**

The procedure for installing a new firmware image is as follows:

1. Connect the serial console available under the service panel.
2. Connect the USB adaptor cable to the mini USB port available under the service panel.
3. Connect the DuraMAR USB-disk key with the adaptor cable.
4. Reboot or switch-on the system.
5. The system will boot from the USB-disk key. While the boot loader is loading the maintenance software, the light on the top of the USB-disk key flashes.
6. When the boot loader has finished loading the maintenance software, the light stops flashing and the boot process begins. From this moment the system activity will be reported with messages on the serial console.
7. At the end of the boot process the maintenance software performs the storage memory partitioning and firmware installation.
8. The installation procedure successfully terminates when the "OK" message appears on the console, otherwise a "KO" message notifies a failure.
9. Disconnect the USB-disk key and restart the system.

In case the installation process fails, the user must repeat the entire procedure.

Using the integrated CISCO router for hosting controller system image files.

Downloading a new image might be quite difficult if the ECC is configured to operate in Bridge Mode. In this configuration the HSDPA interface can't be used by the ECC itself so users, setting the appropriate static routes, must download the new image from a remote host through the slow GPRS interface or from a local host connected to the CISCO Ethernet interface. The latter option is not a viable solution in Dynamic Bridge Mode configuration.

Under these circumstances it might be useful, at first, to download the image file on the flash memory of the CISCO router, that can use the HSDPA interface, and then, make this file available through the IOS integrated HTTP server.

The steps to perform on the CISCO router are:

- Copy from a remote server the image file (.eff) and its MD5 checksum file (.md5). The IOS copy command can copy a file from a remote host using different protocols like HTTP, FTP, TFTP, SSH and RSH.
- Configure and enable the embedded HTTP server:

```
ip http authentication local
ip http path flash:
ip http server
```

- Define a local user with privilege access 15

```
user upgrade secret upgrade
user upgrade privilege 15
```

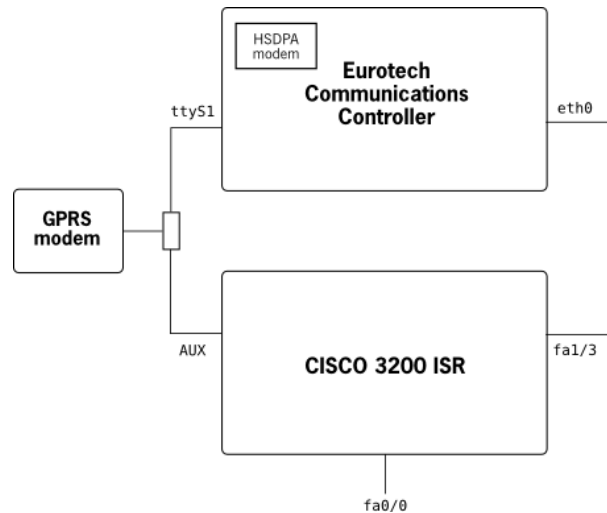
At this point you can install the new system image issuing, on the controller, the upgradefrom command.

For example:

```
upgradefrom http://upgrade:upgrade@ip-address/duramar2150-1.0.1.eff
```

DuraMAR-2150 service interface

A GPRS modem is included as part of the DuraMAR-2150 system in order to provide a diagnostics and backup/emergency connection to the system in the event that the HSDPA link fails.



This GPRS modem has a serial interface and can be connected through a software-controlled switch either to the AUX interface of the CISCO 3200 ISR or to the `ttys1` interface of ECC using a software command or an SMS command message.

The `gprs0` interface is a 2G cellular interface that is mainly targeted for maintenance activity.

This is a special interface because it can be disconnected from the ECC and connected to the AUX port of the CISCO 3200 ISR using a software command. While connected to the ECC, its configuration is similar to the configuration of the `hsdpa0` interface.

While connected with the ECC the GPRS modem is accessible as `gprs0` interface and allows you to establish a PPP connection and to access the device through the Internet.

If switched to the CISCO 3200 ISR, the GPRS modem is accessible and configurable using standard IOS® commands as a modem device connected to the AUX router port.

You can define the device that the GPRS modem is connected with using the command:

```
set gprs cisco | controller
```

The change is immediate; if you want this setup to be permanent, you must save the running configuration issuing the `copy running` command.

The GPRS modem is connected to a dedicated microcontroller that can force a system hardware reset. The reset functions can be asserted in response to a specific SMS command message.

In order for the message to be accepted by the system, it must be sent from a number that is contained in the internal SIM phonebook, messages that are received from unknown numbers are removed from the received message buffer.

The commands are represented by the text of the SMS message. Available commands:

SERCPU	Connects the GPRS modem serial interface to ECC ttyS1 interface
SERCISCO	Connects the GPRS modem serial interface to the AUX port of the CISCO 3200 ISR
RESETCPU	Force a hardware reset of ECC.
RESETALL	Force a complete system reset with power-off/power-on cycling.

When a new SMS message is received, the subscriber number is checked against the available entries in the phonebook and the command is executed only if the number is verified.

Phonebook entries can be managed from ECC CLI using the `set phone-book` command.

The complete syntax of the command is:

```
set phone-book <item> <number>
```

item identifies the entry and must be a number between 1 and 4

number is the authorized subscriber number and must include the international prefix (es. +39)

An item can be removed from the phonebook using the *no-form* of the command. For example the following command will remove the item at position 2:

```
no set phone-book 2
```

In order for the changes to be written to the GPRS modem you must issue a `copy running` command, otherwise any change will be lost after a system restart.

During the execution of this command, the `gprs0` interface must be disabled, otherwise the modem phone-book can't be updated because the interface is in use by the ECC controller.

In case you are using a startup configuration with `gprs0` interface enabled you must:

1. disable the `gprs0` interface first
2. apply changes to the phone-book entries
3. save the running configuration using the `copy running` command
4. enable the `gprs0` interface
5. issue a `copy running` command again

In this case there is no need for accessing the GPRS serial interface during the execution of the `copy running` command because the phone-book is unchanged.

Since the phone-book is loaded from the modem only when system is powered-on, after any change to the phone-book entries the system must be switched off and then switched on again in order for the changes to take effect.



Note:

Wait for about 30 seconds before switching on again

Chapter 4 Environmental and Electrical Specs

Mechanical Characteristics

The enclosure of the DuraMAR-2150 is made of black anodized aluminium, this is secured by two aluminium end-plates which provide the connectors and user interfaces. A grounding terminal is available for connecting the system chassis to the chassis ground of the installation.

Length (mm)	Width (mm)	Height (mm)
254	129	83
Environmental protection class:		IP65

Operating Characteristics

Electrical Operating Characteristics

The system must be powered by a direct current:

Power supply	110Vdc nominal – galvanically isolated
Power consumption	< 44W

**Warning:**

Electric current from power and communication cables is hazardous. To avoid shock hazard when connecting or disconnecting cables, follow appropriate safety precautions. Ensure that the correct operating voltage is used when powering the device.



Danger
110 Volts

Operating Temperature Range

The system can operate in ambient temperature ranges (-20°C/+55°C; +70°C for 10 minutes). The system components are conductively cooled to the enclosure. The DuraMAR-2150 enclosure is convection cooled.

Absolute Maximum Ratings

Storage Temperature Range:	-20°C to +70°C
Non-Condensing Relative Humidity:	<95% at 40°C



Warning: Stressing the device beyond the “Absolute Maximum Ratings” may cause permanent damage. These are stress ratings only. Operation beyond the “Operating Conditions” is not recommended. Extended exposure beyond the “Operating Conditions” may affect device reliability.

Compliance

The system is compliant to the following standards:

Mechanical

Standard	Description
EN-61373	Shock and vibration – applicable to rail and rolling stock installations

Environmental

Standard	Description
EN-50155	Operating temperature range - applicable to rail and rolling stock installations
EN-60068	Environmental testing

Safety

Standard	Description
EN-60950	Safety – applicable to rail and rolling stock installations

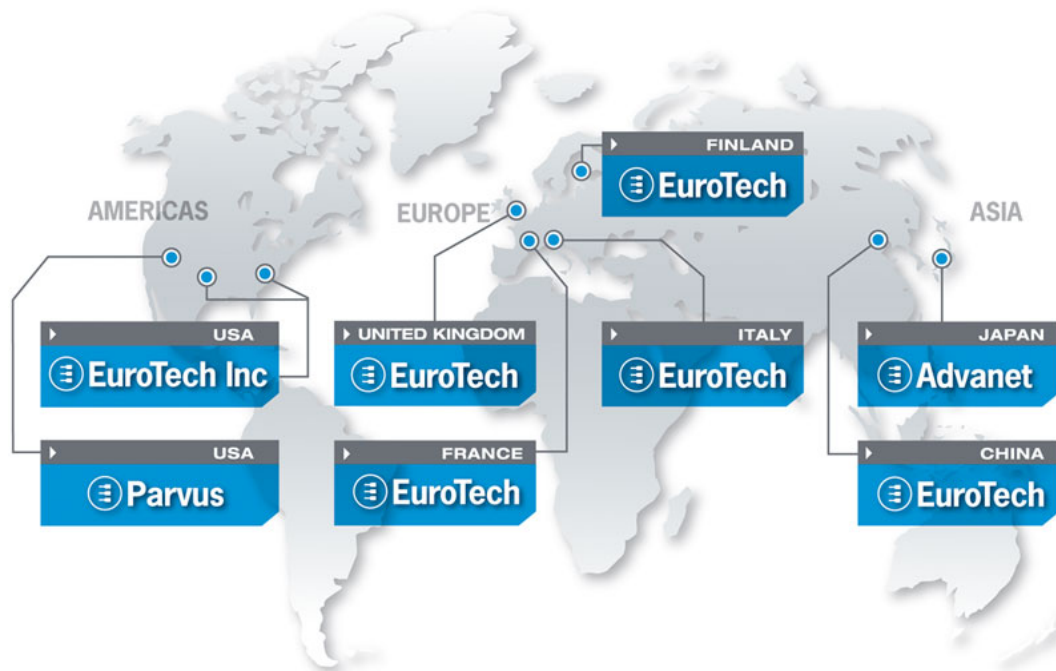
EMC, Immunity and emissions

Global Standard	Description
EN-50155 (including all substandards)	Electrical equipment – applicable to rail and rolling stock installations
EN-55011	Conducted and radiated emissions
EN-61000 (including all substandards)	Immunity
Note:	Sub-standards and alternative naming conventions for EMC standards are included. For more information please contact Eurotech.

Revision History

REVISION	DESCRIPTION	DATE
1.0	First release	December 2008

Eurotech Group Worldwide presence



AMERICAS

EUROPE

ASIA



North America

EUROTECH Inc

toll free +1 888.941.2224
tel. +1 301.490.4007
fax +1 301.490.4582
e-mail: sales-us@eurotech.com
e-mail: support-us@eurotech.com
www.eurotech-inc.com

PARVUS CORPORATION

tel. +1 800.483.3152
fax +1 801.483.1523
e-mail: sales@parvus.com
e-mail: tsupport@parvus.com
www.parvus.com

Central & Southern Europe

EUROTECH Italy

tel. +39 0433.485.411
fax +39 0433.485.499
e-mail: sales-it@eurotech.com
e-mail: support-it@eurotech.com
www.eurotech.com

Western Europe

EUROTECH UK

tel. +44 (0) 1223.403410
fax +44 (0) 1223.410457
e-mail: sales-uk@eurotech.com
e-mail: support-uk@eurotech.com
www.eurotech.com

EUROTECH France

tel. +33 04.72.89.00.90
fax +33 04.78.70.08.24
e-mail: sales-fr@eurotech.com
e-mail: support-fr@eurotech.com
www.eurotech.com

Northern & Eastern Europe

EUROTECH Finland

tel. +358 9.477.888.0
fax +358 9.477.888.99
e-mail: sales-fi@eurotech.com
e-mail: support-fi@eurotech.com
www.eurotech.com

ADVANET Japan

tel. +81 86.245.2861
fax +81 86.245.2860
e-mail: sales@advanet.co.jp
www.advanet.co.jp

EUROTECH China

tel. +86 10.62.67.09.04
fax +86 10.62.67.09.54
e-mail: sales-cn@eurotech.com
e-mail: support-cn@eurotech.com
www.eurotech.com

